IN THE CLAIMS:

1. (Currently Amended) A machine implemented method for multiplying two elements of a finite field that correspond to two input operands, the method comprising the steps of:

mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon the two mapped input operands to produce first result vectors; ~~and~~

performing multiplication of the first result vectors in the ground field using a triangular basis multiplier to produce a multiplier output; and

providing the multiplier output.

2. (Currently Amended) The machine implemented method of claim 1, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming each of the two mapped input operands that each include four sub-elements (a_0, a_1, a_2, a_3) into a respective result vector within the first result vectors that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

3. (Currently Amended) The machine implemented method of claim 1, further comprising the step of performing a final KOA processing of the multiplier output, the final KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

4. (Currently Amended) The machine implemented method of claim 1, further comprising the step of defining the first, second, and third irreducible polynomials.

5. (Currently Amended) A machine implemented method for multiplying two elements of a finite field that correspond to two input operands, the method comprising the steps of:

mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon each of the two mapped input operands to produce first result vectors, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; ~~and~~

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field; and

providing the multiplicative product as an output.

6. (Currently Amended) The machine implemented method of claim 5, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

7. (Currently Amended) The machine implemented method of claim 5, further comprising the step of defining the first, second, and third irreducible polynomials.

8. (Currently Amended) A hardware implemented Galois field multiplier comprising:

an input operand mapper for mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

an initial KOA processor for performing an initial KOA processing upon the two mapped input operands to produce first result vectors; ~~and~~

a triangular basis ground field multiplier for performing multiplication in the ground field to produce a multiplier output; and

an output for providing the multiplier output.

9. (Currently Amended) The hardware implemented Galois field multiplier of claim 8,

wherein the initial KOA processor transforms each of the two mapped input operands that each include four sub-elements (a_0, a_1, a_2, a_3) into a respective result vector within the first result vectors that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

10. (Currently Amended) The hardware implemented Galois field multiplier of claim 8, further comprising a final KOA processor for performing a final KOA processing of the multiplier output, the final KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

11. (Currently Amended) The hardware implemented Galois field multiplier of claim 8, wherein the first, second, and third irreducible polynomials are used-defined.

12. (Currently Amended) A hardware implemented finite field data multiplier for multiplying two elements of a finite field that correspond to two input operands, the multiplier comprising:

an input operand mapper for mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

an initial KOA processor for performing an initial KOA processing upon each of the two mapped input operands to produce first result vectors, the initial KOA processor dividing the mapped input operands into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; ~~and~~

a multiplier means for performing a subsequent multiplication processing upon a result from the initial KOA processor to produce a multiplicative product over the composite finite field; and

a multiplier output for providing the multiplicative product.

13. (Currently Amended) The hardware implemented multiplier of claim 12, wherein the initial KOA processor produces a plurality of output operands that each are within the ground field.

14. (Currently Amended) The hardware implemented multiplier of claim 12, wherein the first, second, and third irreducible polynomials are used-defined.

15. (Previously Presented) A machine-readable medium encoded with a program for multiplying two elements of a finite field that correspond to two input operands, said program containing instructions for performing the steps of:

mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon the two mapped input operands to produce first result vectors; ~~and~~

performing multiplication of the first result vectors in the ground field using a triangular basis multiplier to produce a multiplier output; and

providing the multiplier output.

16. (Previously Presented) The machine-readable medium of claim 15, wherein the step of performing the initial KOA processing includes the sub-step of:

transforming each of the two mapped input operands that each include four sub-elements (a_0, a_1, a_2, a_3) into a respective result vector within the first result vectors that is defined by:

$$\begin{pmatrix} a_0 \\ a_0 + a_1 \\ a_1 \\ a_0 + a_2 \\ \text{----} \\ a_0 + a_1 + a_2 + a_3 \\ a_1 + a_3 \\ a_2 \\ a_2 + a_3 \\ \text{--------} \\ a_3 \\ x \\ x \\ x \end{pmatrix}$$

wherein the "+" operator represents a bit-wise exclusive-OR operation and "x" indicates unused or undefined values.

17. (Previously Presented) The machine-readable medium of claim 15, wherein said program further contains instructions for performing the step of performing a final KOA processing of the multiplier output, the final KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field.

18. (Previously Presented) A machine-readable medium encoded with a program for multiplying two elements of a finite field that correspond to two input operands, said program containing instructions for performing the steps of:

mapping two input operands into two mapped input operands in a composite finite field that is defined by a first irreducible polynomial of degree m*n, the first irreducible polynomial being defined by using a ground field that is defined by a second irreducible polynomial of degree n and by using an extension field that is defined by a third irreducible polynomial of degree m;

performing an initial KOA processing upon each of the two mapped input operands to produce first result vectors, the initial KOA processing being divided into a plurality of uniform subsets such that the uniform subsets are scalable for processing of different values of m used to define the extension field; ~~and~~

performing a subsequent multiplication processing upon a result of the initial KOA processing to produce a multiplicative product over the composite finite field; and

providing the multiplicative product as an output.

19. (Original) The machine-readable medium of claim 18, wherein the step of performing the initial KOA processing includes the sub-step of producing a plurality of output operands that each are within the ground field.

20. (Currently Amended) A machine implemented method for multiplying two elements corresponding to a first multiplicand and a second multiplicand of a finite field, with an initial basis, that is redefinable, the method comprising the steps of:

switching data bit ordering of a plurality of data bits representing a first multiplicand to produce a first bit switched multiplicand, such that a most significant bit of the first multiplicand is placed into a least significant bit position regardless of the number of bits in the plurality of data bits representing the first multiplicand, successively less significant bits are placed into successively more significant bit positions relative to the least significant bit position, and unused bits are set to zero;

converting the first bit switched multiplicand from the initial basis into a triangular basis;

switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, such that a most significant bit of each of the coefficients is placed into a least significant bit position regardless of the number of bits in the plurality of coefficient bits, successively less significant bits are placed into successively more significant bit positions relative to the least significant bit position, and unused bits are set to zero;

performing multiplication based upon at least the first bit switched multiplicand in the triangular basis and a second multiplicand that is converted from the initial basis to the triangular basis to produce a multiplication result; ~~and~~

converting the multiplication result from ~~that is converted from the initial basis to~~ the triangular basis ~~triangular basis~~ to the initial basis to produce a multiplier output; and

providing the multiplier output.

21. (Currently Amended) The machine implemented method of claim 20, wherein the step of performing multiplication includes the sub-steps of:

generating a Hankel Matrix based upon the first multiplicand and the plurality of coefficients; and

multiplying the Hankel matrix with a second multiplicand to produce the multiplication result.

22. (Currently Amended) The machine implemented method of claim 20, wherein the step of switching data bit ordering of a plurality of data bits includes the step of selecting a plurality of outputs from a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

23. (Original) A machine-readable medium encoded with a program for performing the method of claim 20.

24. (Currently Amended) A hardware implemented flexible Galois field multiplier for multiplying two elements corresponding to a first multiplicand and a second multiplicand of a finite field, with an initial basis, that is redefinable, the multiplier comprising:

a first switching circuit for switching data bit ordering of a plurality of data bits representing a first multiplicand to produce a first bit switched multiplicand, the first switching circuit placing a most significant bit of the first multiplicand into a least significant bit position regardless of the number of bits in the plurality of data bits representing the first multiplicand, placing successively less significant bits into successively more significant bit positions relative to the least significant bit position, and setting unused bits to zero;

a first basis converter for converting the first bit switched multiplicand from an initial basis into a triangular basis;

a second switching circuit for switching data bit ordering of a plurality of coefficient bits representing each of a plurality of coefficients in a Galois Field generator polynomial that defines a Galois Field over which multiplication is to be performed, the second switching circuit placing a most significant bit of each of the coefficients into a least significant bit position regardless of the number of bits in the plurality of coefficient bits, placing successively less significant bits into successively more significant bit positions relative to the least significant bit position, and setting unused bits to zero;

a multiplier for performing multiplication based upon at least the first bit switched multiplicand in the triangular basis and a second multiplicand that is converted from the initial basis to the triangular basis to produce a multiplication result; ~~and~~

a second basis converter for converting the multiplication result from the triangular basis to the initial basis; and

an output for providing the multiplication result in the initial basis.

25. (Currently Amended) The hardware implemented multiplier of claim 24, wherein the multiplier generates a Hankel Matrix based upon the first multiplicand and the plurality of coefficients, and multiplies the Hankel matrix with a second multiplicand to produce the multiplication result.

26. (Currently Amended) The hardware implemented multiplier of claim 24, wherein the first switching circuit includes a plurality of data multiplexers, the plurality of data multiplexers including one data multiplexer for each data bit in the plurality of data bits.

27-32. (Canceled)